从 Cisco Meeting Server 2.9 平稳升级至 3.0（及更高版本）指南

目录

简介

本文档介绍将运行版本2.9（或更低版本）的思科Meeting Server部署升级到3.0（或更高版本）所面临的挑战，以及如何处理这些挑战以实现平稳升级过程。

删除的功能：删除XMPP（影响WebRTC）、中继/负载均衡器、Webbridge

功能更改：录制器和流转换器现在是SIP，webbridge替换为webbridge3

本文档仅介绍在升级之前需要考虑的主题。它并未涵盖3.X中的所有新功能。

先决条件

要求

Cisco 建议您了解以下主题：

- CMS管理
- CMS升级
- 证书创建和签名

这里提到的所有内容在各种文件中都有介绍。 如需有关功能的更多说明，请务必阅读产品发行版本注释，并参阅我们的编程指南和部署指南：CMS安装和配置指南和CMS产品发行版本注释。

使用的组件

本文档中的信息基于思科Meeting Server。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档旨在指导您是否已部署CMS 2.9.x（或更早版本），无论是否单一组合或具有恢复能力，也不管您计划何时升级到CMS 3.0。 本文档中的信息涉及所有CMS型号。

注意：X系列无法升级到CMS 3.0。您需要计划尽快更换X系列服务器。

有关升级的重要信息

唯一支持的CMS升级方法是逐步升级。 在撰写本文时，CMS 3.5已发布。 如果您使用的是CMS 2.9，则必须以阶梯式方式升级(2.9 —> 3.0 —> 3.1 —> 3.2 —> 3.3 —> 3.4 —> 3.5(注意，升级过程自CMS 3.5起已更改，因此请仔细阅读版本说明!!)

如果您不执行分步升级，并且遇到异常行为，TAC可能会请求您降级并重新开始。

此外，从CMS 3.4开始，CMS必须使用智能许可。 您不能升级到CMS 3.4或更新版本，仍使用传统许可证。 除非已设置智能许可，否则请勿升级到CMS 3.4或更高版本。

要考虑的事项摘要

使用这些问题导航至与您自己的情况有关的部分。 每个注意事项都指向一个超链接，指向本文档中提供的更详细的说明。

许可证

在升级之前，您的服务器上是否有足够的个人多方(PMP)/共享多方(SMP)许可证？

在3.0中，即使用户未登录，也会分配PMP许可证。例如，如果您通过LDAP导入了10000个用户，但您只有100个PMP许可证，则一旦升级到3.0，就会使您不符合要求。 对于此使用案例，请确保检查已设置userProfile和/或system/profiles的租户，以查看是否设置了值为true的userProfile with hasLicense。

本节将详细介绍如何检查API上的userProfile并查看您是否设置了hasLicense=true（表示PMP许可用户）。

您当前的cms.lic文件中是否有PMP/SMP许可证？

由于3.0之后的许可证行为更改，在执行升级之前，您必须确认是否具有足够的PMP/SMP许可证。本部分对此进行了更详细的说明。

您是否部署了思科Meeting Manager (CMM)？

CMS 3.0需要CMM 3.0，因为处理许可证的方式发生了变化。建议您在执行环境升级到3.0之前部署CMM 2.9，因为您可以检查过去90天的90天许可证使用情况报告。本部分对此进行了更详细的说明。

您是否有智能许可？

CMS 3.0需要CMM 3.0，因为处理许可证的方式发生了变化。因此，如果您已经通过CMM使用智能许可，请确保您已将PMP和SMP许可证关联到集群。

Webbridge（WebRTC和CMA客户端）

您是否在CMS 2.9中使用WebRTC？

CMS 3.0中的Webbridge发生了重大变化。 有关从Webbridge2迁移到Webbridge3以及使用Web应用的指导，请参阅此部分。

您的用户是否使用CMA胖客户端？

由于这些客户端是基于XMPP的，因此升级后无法再使用这些客户端，因为XMPP服务器已被删除。如果这对您的使用案例适用，您可以在此部分找到详细信息。

您是否在WebRTC中使用聊天？

在3.0中，聊天功能已从Web应用中删除。在CMS 3.2中，聊天功能重新引入，但并非持久聊天。您可以在此部分找到有关此功能的详细信息。

您的用户是否执行从WebRTC到设备的点对点呼叫？

在CMS 3.0中，Web应用用户无法再直接拨号到其他设备。现在，您必须加入会议空间，并有权限向会议添加参与者，以便执行相同的操作。 在此部分中可以找到有关此部分的更多信息。

您的用户是否从WebRTC创建自己的coSpaces？

在3.0中，为了使Web应用用户能够从客户端创建自己的空间，需要在API中创建coSpaceTemplate并将其分配给用户。在LDAP导入过程中，此操作可以是手动或自动的。CanCreateCoSpaces已从UserProfile中删除。 您可以在此部分找到有关此功能的详细信息。

Web GUI更改

您是否在Web管理GUI中配置了WebBridge设置？

在3.0中，WebBridge设置会从GUI中删除，因此您必须在API中配置WebBridge，并注意GUI中的当前设置，以便在API中相应地配置WebBridgeProfiles。 您可以在此部分找到有关此更改的详细信息。

您是否在Web管理GUI中配置了External Settings？

外部设置已从CMS 3.1的GUI中删除。 如果您在CMS 3.0或更早版本的Web管理GUI（配置—>常规—>外部设置）中配置了Webbridge URL或IVR，则这些设置已从网页中删除，现在需要在API中进行配置。升级到3.1之前的设置不会添加到API中，必须手动完成。 您可以在此部分找到有关此更改的详细信息。

记录器/流转换器

您当前是否使用任何CMS录制器和/或流转换器？

CMS录制器和流转换器组件现在基于SIP，而不是基于XMPP。因此，在删除XMPP时，需要在升级后对这些进行微调。您可以在此部分找到有关此更改的详细信息。

Cisco Expressway注意事项

如果您使用Expressway代理WebRTC，您当前的Cisco Expressway版本是多少？

CMS 3.0需要Expressway 12.6或更高版本。 您可以在此部分找到有关此WebRTC代理功能的详细信息。

CMS边缘

您的环境中当前是否有CMS Edge？

CMS Edge在CMS 3.1上重新引入，具有更高的外部连接可扩展性。 在此部分中可以找到有关此部分的更多信息。

CMS (Acano) X系列

您的环境中当前是否有x系列服务器？

这些服务器无法升级到CMS 3.0，您必须考虑尽快更换这些服务器（在升级到3.0之前迁移到虚拟机或CMS设备）。在此链接中可以找到有关这些服务器的寿命终止通知。

SIP边缘

您当前是否在您的环境中使用SIP Edge？

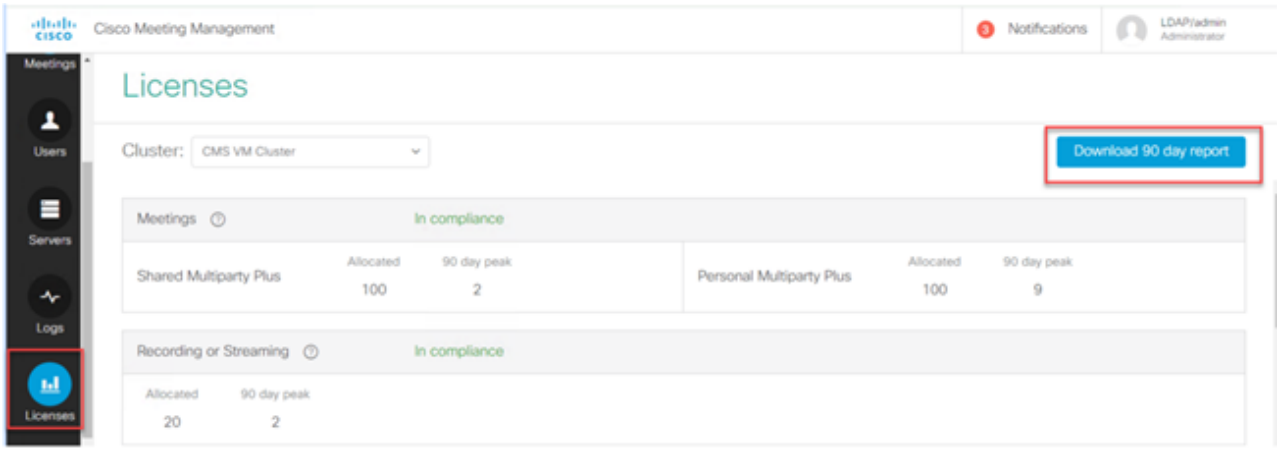
从CMS 3.0开始，Sip Edge已完全弃用。 您需要使用Cisco Expressway将SIP呼叫引入您的CMS。请与您的思科客户代表联系，了解如何为您的组织获取Expressway。

更多信息

许可-升级前检查许可证

从2.x版本升级到3.0或更高版本时，许可证状态不合规(out of compliance)是最严重的问题。本节介绍如何确定平稳升级所需的PMP/SMP许可证数量。

在将部署升级到3.0之前，请部署CMM 2.9，并检查Licenses 选项卡下的90天报告，以查看许可证使用量是否一直低于您当前在CMS节点上分配的许可证数量：

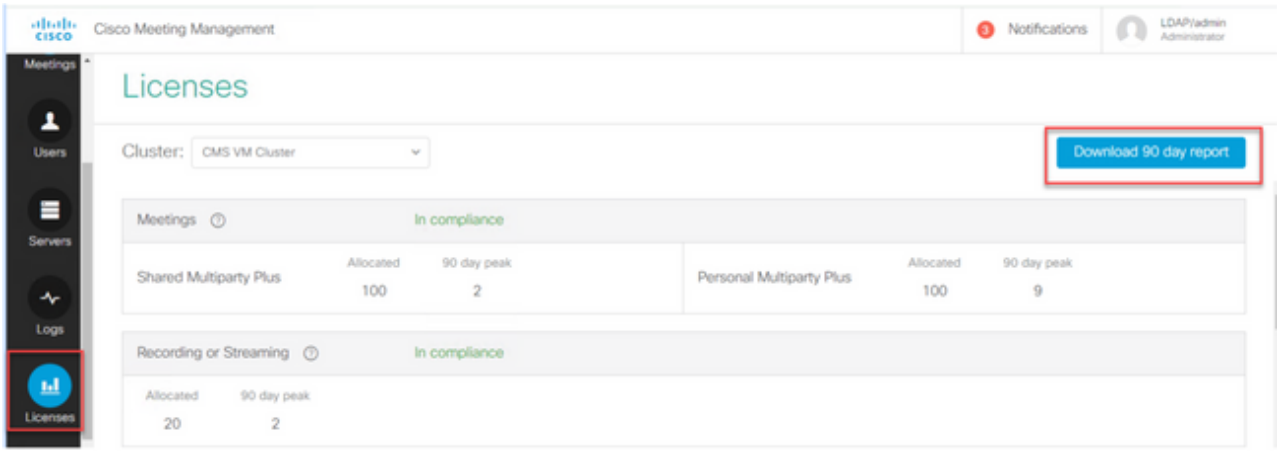


如果您使用传统许可（cms.lic文件在您的CMS节点上本地安装），请查看CMS许可证文件以了解每个CMS节点上的个人和共享许可证数量（根据本处的映像，为100/100个）（从每个callBridge节点通过WinSCP下载）。

```
    ],
    "issued_to": "Darren McKinnon - TAC",
    "notes": "Darren McKinnon - TAC",
    "features":
    {
        "callbridge":
        {
            "expiry": "2100-Jan-03"
        },
        "webbridge3":
        {
            "expiry": "2100-Jan-03"
        },
        "customizations":
        {
            "expiry": "2100-Jan-03"
        },
        "recording":
        {
            "expiry": "2100-Jan-03",
            "limit": "10"
        },
        "personal":
        {
            "expiry": "2100-Jan-03",
            "limit": "100"
        },
        "shared":
        {
            "expiry": "2100-Jan-03",
            "limit": "100"
        },
        "streaming":
        {
            "expiry": "2100-Jan-03",
```


如果您已使用智能许可，请检查在思科软件智能门户中为CMS服务器分配了多少PMP/SMP许可证。

许可证相关的问题，但如果您检查90天峰值，发现您使用的许可证多于可用许可证数量，则您仍可以升级到CMS 3.0并使用CMM上的90天试用许可证，以便使用您的许可进行问题解决，或在升级之前采取行动。



配置Webbridge（WebRTC和CMA客户端）

CMS 3.0移除XMPP服务器组件，并随之移除WebBridge和使用CMA胖客户端的能力。 WebBridge3现在用于通过浏览器将Web应用用户（以前称为WebRTC用户）连接到会议。 升级到3.0时，需要配置Webbridge3。

注意：升级到CMS 3.0后，CMA胖客户端无法正常工作！

此视频会引导您完成有关如何创建Webbridge 3证书的过程。

https://video.cisco.com/detail/video/6232772471001?autoStart=true&q=cms

在升级到3.0之前，客户必须计划如何配置Webbridge3。此处重点介绍最重要的步骤。

1. Webbridge3确实需要密钥和证书链。 如果证书包含运行Webbridge3的所有CMS服务器FQDN或IP地址作为主题备用名称(SAN)/公用名(CN)，并且满足以下条件之一，则可以使用旧的Webbridge证书：

a.证书没有增强的密钥用法（意味着它可以用作客户端或服务器）。

b.证书同时具有客户端和服务器身份验证。 HTTPs证书实际上只需要服务器身份验证，而C2W证书需要服务器和客户端)。

2. 如果要为“webbridge3 https”证书创建新证书，建议公开签名（以避免使用Web应用时在客户端上出现证书警告）。 此相同的证书可用于“webbridge3 c2w证书”，并且证书必须具有SAN/CN中Webbridge服务器的FQDN。

3. CallBridge需要使用在webbridge3 c2w listen命令中配置的端口与新的webbridge3通信。这可以是任何可用端口，例如449。用户需要确保Callbridge可以与此端口上的Webbridge3通信，并在必要时提前更改防火墙。 它不能是“webbridge https”用于侦听的同一端口。

在CMS升级到3.0之前，建议使用“backup snapshot <servername_date>”进行备份，然后登录

Callbridge节点上的Webadmin页面，以删除所有XMPP设置和Webbridge设置。 然后连接到服务器上的MMP，并通过SSH连接对具有xmpp和webbridge的所有核心服务器执行以下步骤：

1. xmpp disable
2. XMPP重置
3. xmpp certs none
4. xmpp domain none
5. webbridge disable
6. webbridge listen none
7. webbridge证书无
8. webbridge trust none

升级到3.0后，首先在以前运行Webbridge的所有服务器上配置Webbridge3。 您必须执行此操作，因为已经存在指向这些服务器的DNS记录，因此，您可以确保如果用户被发送到Webbridge3，它将准备好处理请求。

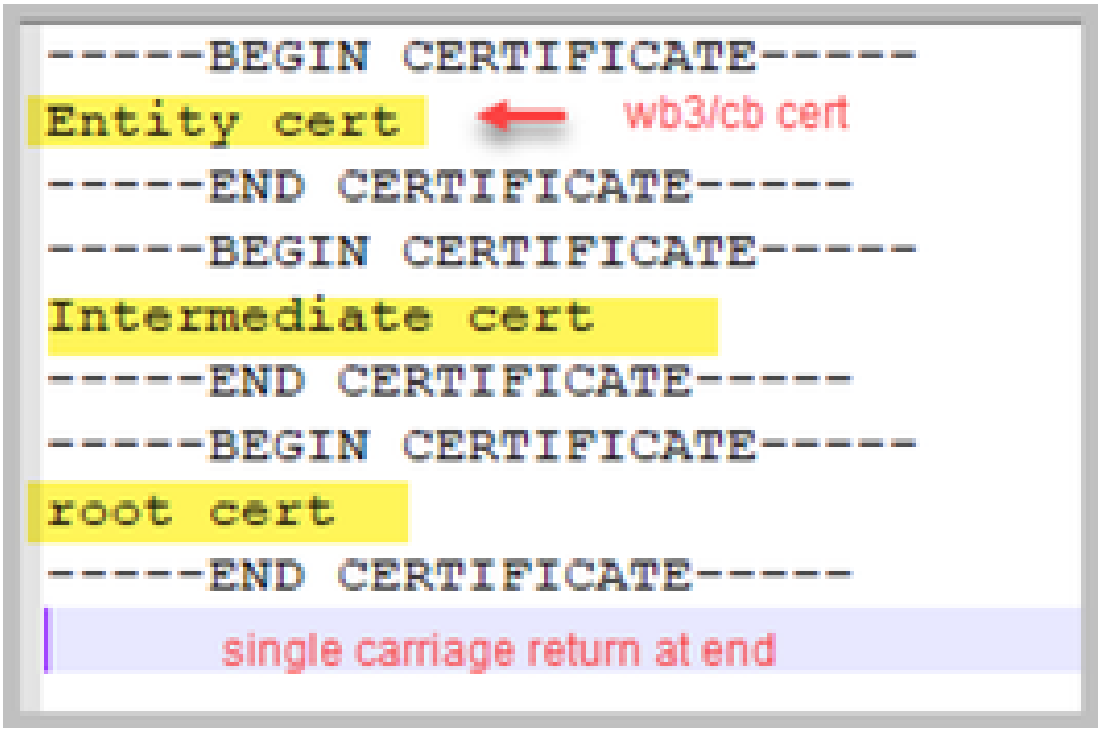
Webbridge3配置（全部通过SSH连接）

步骤1:配置webbridge3 http侦听端口。

Webbridge3 https listen a：443

第二步：为浏览器连接的webbridge3配置证书。 这是发送到浏览器的证书，需要由公共证书颁发机构(CA)签署，并包含浏览器中使用的FQDN以使浏览器信任连接。

Webbridge3 https certs wb3.key wb3trust.cer（这必须是信任链：按顺序制作具有终端实体的信任证书，然后是中间CA，最后使用RootCA）。



第三步：配置用于侦听callBridge到Webbridge (c2w)连接的端口。 由于443用于webbridge3 https侦听端口，因此此配置必须是不同的可用端口，例如449。

Webbridge3 c2w listen a：449

4. 为c2w信任配置Webbridge发送到Callbridge的证书

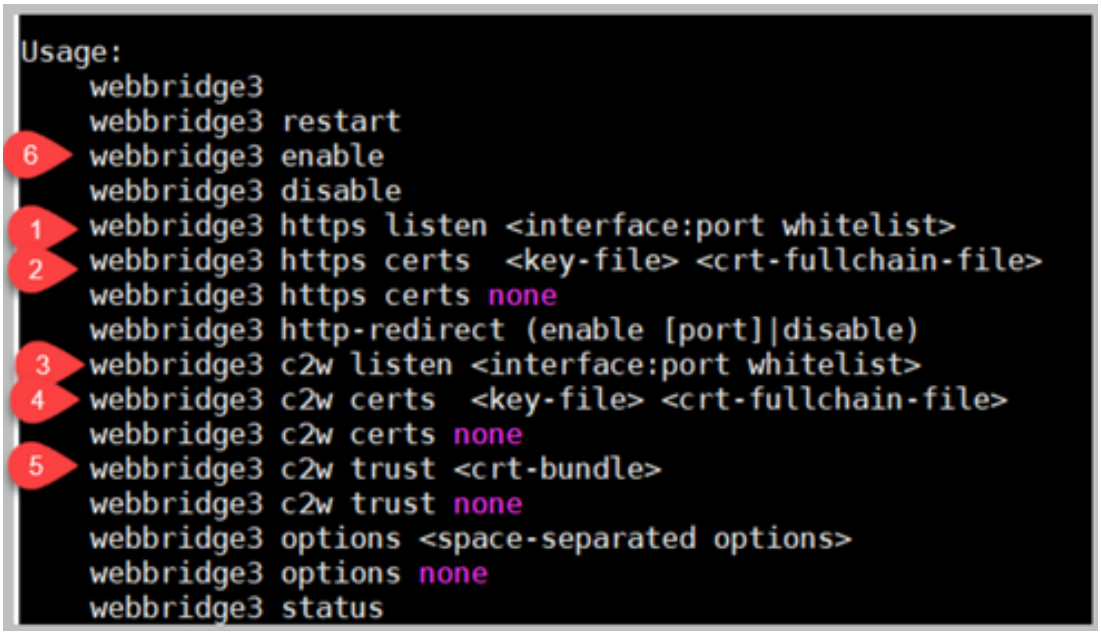
Webbridge3 c2w certs wb3.key wb3trust.cer

5. 配置WB3用于信任callBridge证书的信任库。 这必须与Callbridge CA捆绑包上使用的证书相同（并且必须是中间证书的捆绑包，在末尾的根CA后面是单回车符）。

Webbridge3 c2w trust rootca.cer

6. 启用Webbridge3

Webbridge3 enable



CallBridge配置更改（全部通过SSH连接）

步骤1:使用签署Webbridge3 c2w证书的CA证书/捆绑包配置callBridge信任。

Callbridge trust c2w rootca.cer

第二步：重新启动callBridge以使新信任生效。 这将丢弃此特定callBridge上的所有呼叫，因此请谨慎使用此选项。

Callbridge重启

用于连接webBridge3的callBridge的API配置

1. 使用API中的POST创建新的WebBridge对象，并使用在Webbridge c2w接口白名单中配置的FQDN和端口为其提供URL值（webbridge3配置中的步骤3）

c2w://webbridge.darmckin.local:449

此时，Webbridge3将再次运行，您可以作为访客加入空间，或者如果您以前导入过用户，他们必须

能够登录。

Web应用用户空间创建权限

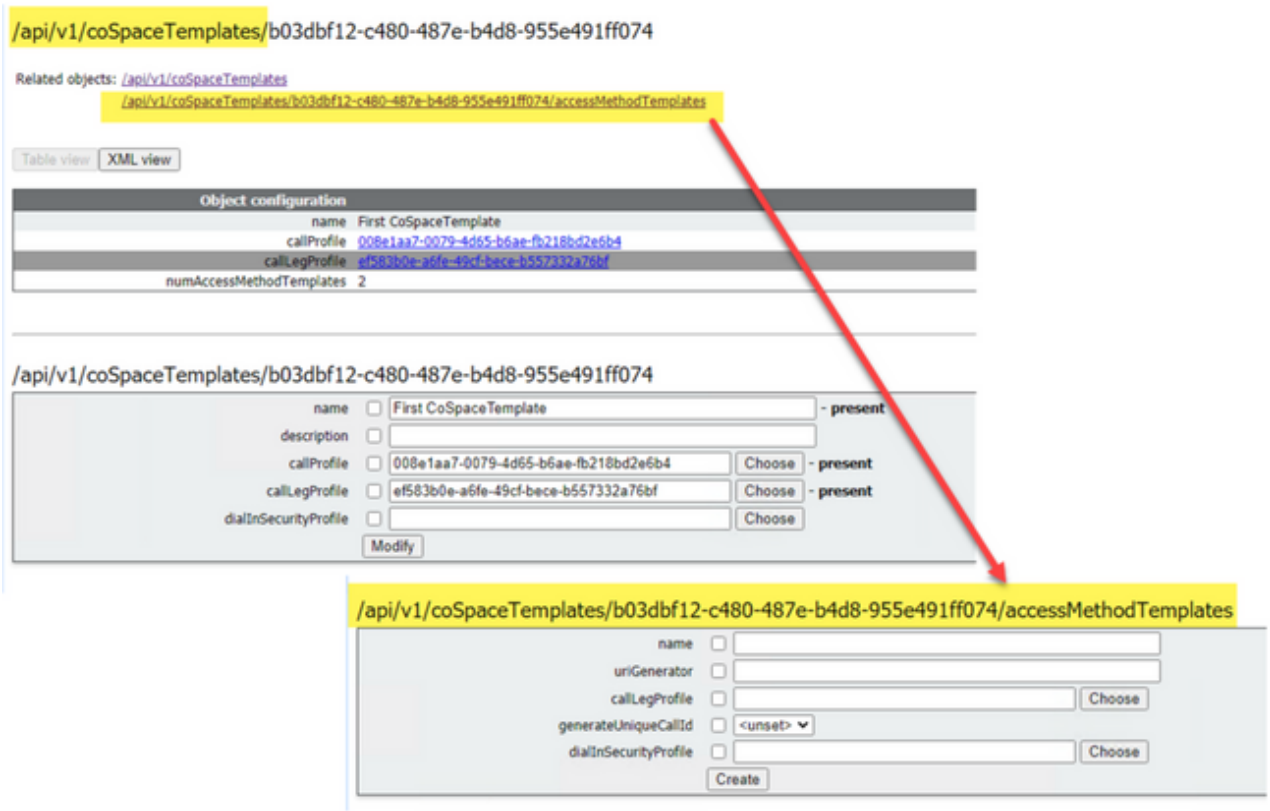
您的用户是否习惯了在WebRTC中创建自己的空间？ 从CMS 3.0开始，Web应用用户无法创建自己的coSpaces，除非他们分配了一个允许创建自己的coSpace模板。

即使分配了coSpaceTemplate，这也不会创建其他人可以拨入的空间（无URI、无呼叫ID或密码），但如果coSpace具有带“addParticipantAllowed”的callLegProfile，则他们可以从空间拨出。

为了使用拨号字符串来呼叫新空间，coSpaceTemplate必须具有accessMethodTemplate设置(请参阅2.9发行说明-https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-2-9/Cisco-Meeting-Server-Release-Notes-2-9-6.pdf)。

在API中，创建coSpaceTemplate(s)，然后创建accessMethodTemplate(s)，并将coSpaceTemplate分配给ldapUserCoSpaceTemplateSources，也可以手动将coSpaceTemplate分配给api/v1/users中的用户。

您可以创建并分配多个CoSpaceTemplates和accessMethodsTemplates。 有关详细信息，请参阅CMS API指南(https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html)



CoSpaceTemplate（API配置）

Name：要为coSpaceTemplate指定的任何名称。

说明：简要说明（如果需要）。

callProfile：是否希望使用此模板创建的任何空间使用White callProfile？如果未提供，则使用在系统/配置文件级别设置的内容。

calllegProfile：您希望使用此模板创建的任何空间使用哪个calllegProfile？ 如果未提供，则使用在系统/配置文件级别设置的内容。

dialInSecurityProfile：您希望使用此模板创建的任何空格使用哪个dialInSecurityProfile？如果未提供，则使用在系统/配置文件级别设置的内容。

AccessMethodTemplate（API配置）

Name：要为coSpaceTemplate指定的任何名称。

uriGenerator：用于为此访问方法模板生成URI值的表达式；允许的字符集为'a'到'z'、'A'到'Z'、'0'到'9'、'.'、'-'、'_'和'$'；如果不为空，则它必须正好包含一个'$'字符。 例如，$.space在创建空间时使用用户提供的名称并附加“.space”。“团队会议”会创建url“Team.Meeting.space@domain”。

callLegProfile：您希望使用此模板创建的任何访问方法使用哪个calllegProfile？ 如果未提供，它将使用所设置的CoSpaceTemplate级别，如果没有，则使用系统/配置文件级别中的内容。

generateUniqueCallId：是否为此访问方法生成唯一数字ID，这会覆盖cospace的全局数字ID。

dialInSecurityProfile：您希望使用此模板创建的任何访问方法使用哪个dialInSecurityProfile？如果未提供，它将使用所设置的CoSpaceTemplate级别，如果没有，则使用系统/配置文件级别中的内容。

聊天功能

CMS 3.0删除了持续聊天功能，但在CMS 3.2中返回了空间内的非持续聊天。 Web应用用户可以使用“聊天”，但聊天不会存储在任何位置。 安装CMS 3.2后，Web应用用户默认能够在会议期间相互发送消息。 这些消息仅在会议期间可用，并且只能看到加入后交换的消息。您不能延迟加入和滚动回来查看以前的消息。

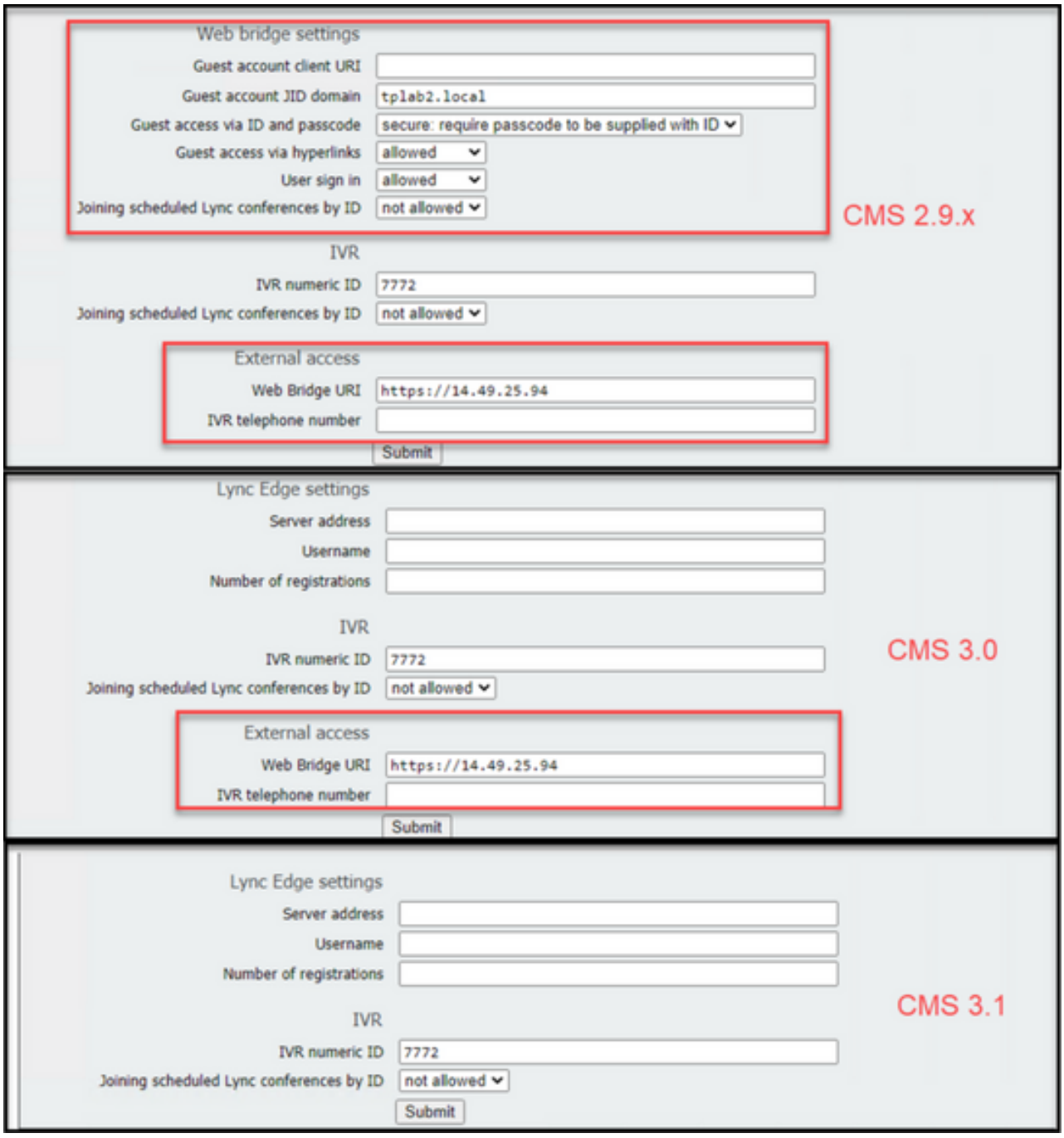
WebRTC点对点呼叫

在CMS 2.9.x上，WebRTC参与者可以从其客户端直接拨打其他联系人。 从CMS 3.0开始，此操作不再可行。现在，用户必须登录并加入空间。如果他们在那里有callLegProfile(将addParticipants参数设置为True)的权限，则他们可以添加其他联系人。 这会使CMS向参与者拨号，并且参与者在CMS中的空间上开会。

值得注意的WebBridge设置更改

CMS 3.0和3.1已从GUI中删除或重新调整了某些Webbridge设置，需要在API中进行配置以保持用户的一致体验。 在3.x上，使用api/v1/webBridge和api/v1/webBridgeProfiles。

检查您当前已配置的内容，这样，在升级到3.0时，您可以相应地在API中配置Webbridge和Webbridge配置文件。

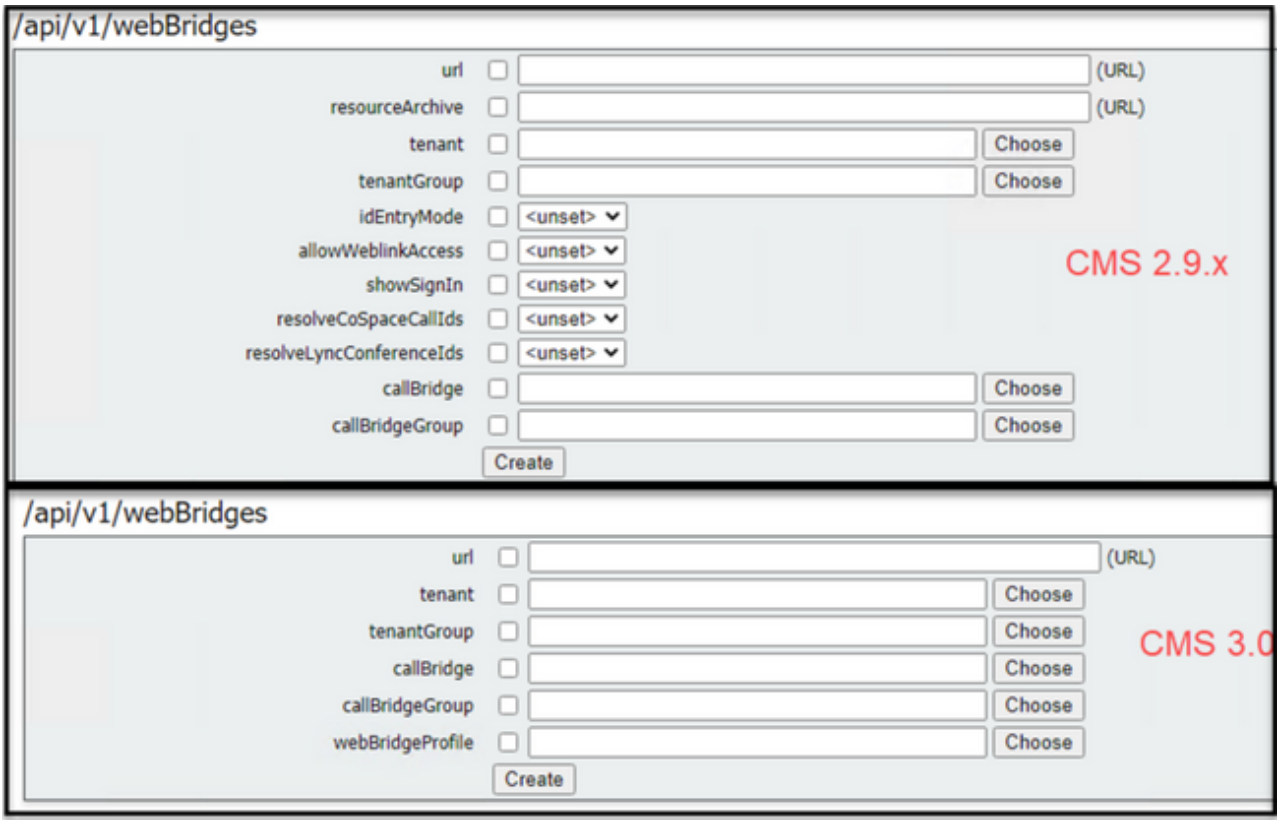


在3.0中，在GUI上删除了Web网桥设置，然后在CMS 3.1中，外部访问字段也已删除。

GUI中的Web网桥设置

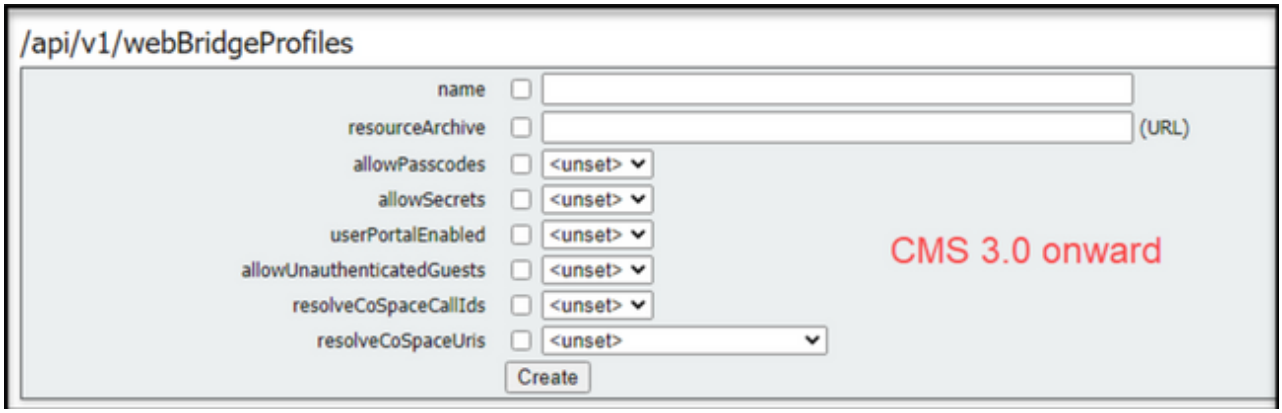
- 访客账户客户端URI - callBridge用它来查找WebBridge。 如果在部署中为WebRTC部署了多个WebBridge，则此字段必须为空，并且对于callBridge需要连接的每个WebBridge，必须在api/v1/WebBridge中具有唯一URL。 删除此字段中的任何内容，并确保您在API中配置了webBridge。

- 访客帐户Jid域 - CMS 3.0中不再使用此域，您可以删除它。
- 访客通过ID和密码访问 -在CMS 3.0中删除且未替换。
- 通过超链接进行的访客访问- 现在可在API中的webBridgeProfiles下设置“AllowSecrets”中进行配置。



注意，在CMS 3.0中，已从api/v1/webBridge中删除多个字段。

- resourceArchive -现已在webbridgeProfiles中。
- idEntryMode - 现已弃用。
- allowWeblinkAccess -现已在webBridgeProfiles中作为allowSecrets。
- showSignin - 现在在webBridgeProfiles中作为userPortalEnabled。
- resolveCoSpaceCallIds- 现已在webbridgeProfiles中。
- resolveLyncConferenceIDs - 现在位于webbridgeProfiles中。



Web网桥配置文件

- resourceArchive -如果您使用自定义背景并且资源存档存储在Web服务器上，请在此处输入URL。
- allowPasscodes -如果为false，则用户没有作为访客加入会议的选项。 他们只能登录或使用包含空间信息和密钥的URL
- allowSecrets - 如果设置为false，则用户无法使用

https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_I.zw等URL加入空格。用户需要使用https://meet.company.com，并输入呼叫ID/会议ID/URI和PIN/密码（如果已配置）。

- userPortalEnabled -如果设置为false，则Web应用门户登录页不显示登录选项。它仅显示用于输入呼叫ID/会议ID/URI和PIN/密码（如果已配置）的字段。
- allowUnauthenticatedGuests - 如果设置为False，则访客无法加入任何会议-即使具有包含会议ID和密钥的完整URL。 如果为False，则只有可以登录的用户才能加入会议。 示例。User2正在尝试使用User1会议的URL。 输入URL后，User2必须登录才能继续参加User1的会议。
- resolveCoSpaceCallIds -如果设置为False，则访客只能通过输入URI和PIN/密码（如果使用）来加入会议。 不接受呼叫ID/会议ID/数字ID。
- resolveCoSpaceUri - 3个可能的设置：off、domainSuggestionDisabled和domainSuggestionEnabled。此webBridge是否接受coSpace和coSpace accessMethod SIP URI，以便允许访问者加入cospace会议。

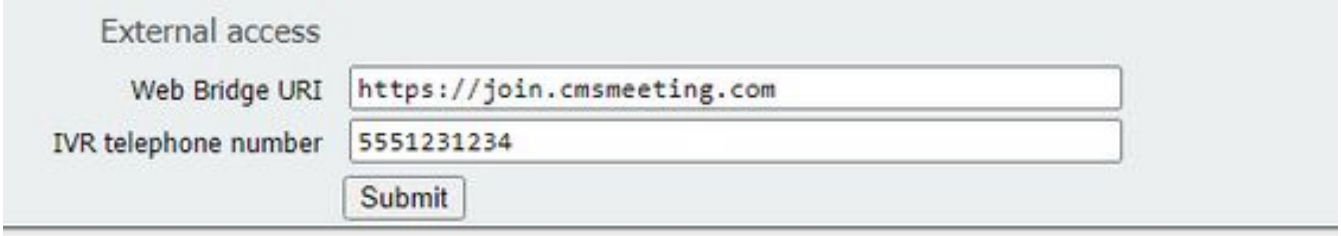
- 设置为“off”时，将禁用通过URI加入。

- 设置为domainSuggestionDisabled时，通过URI加入处于启用状态，但该URI的域未自动完成或在使用此webBridgeProfile的webBridge上验证。

- 如果设置为“domainSuggestionEnabled”，则通过URI的加入处于启用状态，并且可以在使用此webBridgeProfile的webBridge上自动完成并验证URI的域。

从Web GUI中删除的外部访问部分

在CMS 3.1中，“外部访问”部分已从Web GUI中删除。如果您在升级前已配置这些部分，则需要在WebbridgeProfiles下的API中重新配置它们。



首先，您需要创建一个WebbridgeProfile，如上一节所述。创建WebbridgeProfile后，可以通过新创建的WebBridgeProfile下API中可用的链接创建IVR号码和/或Web网桥URI。

您可以创建多达32个IVR号码或每个WebBridgeProfile 32个WebbridgeAddresses

录制或流

CMS 2.9.x和更早版本上的录制器和流转换器组件是XMPP客户端，从CMS 3.0开始，它们基于SIP。 现在，这允许使用API中的默认布局更改录制和流传输的布局。此外，现在名称标签显示在录制/流传输会话中。 有关录制器/流传输功能的详细信息，请参阅CMS 3.0发行说明- https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-3-0/Cisco-Meeting-Server-Release-Notes-3-0.pdf。

如果您在2.9.x中配置了recorder或streamer，则需要重新配置MMP和API中的设置，以便升级后这些设置继续工作。

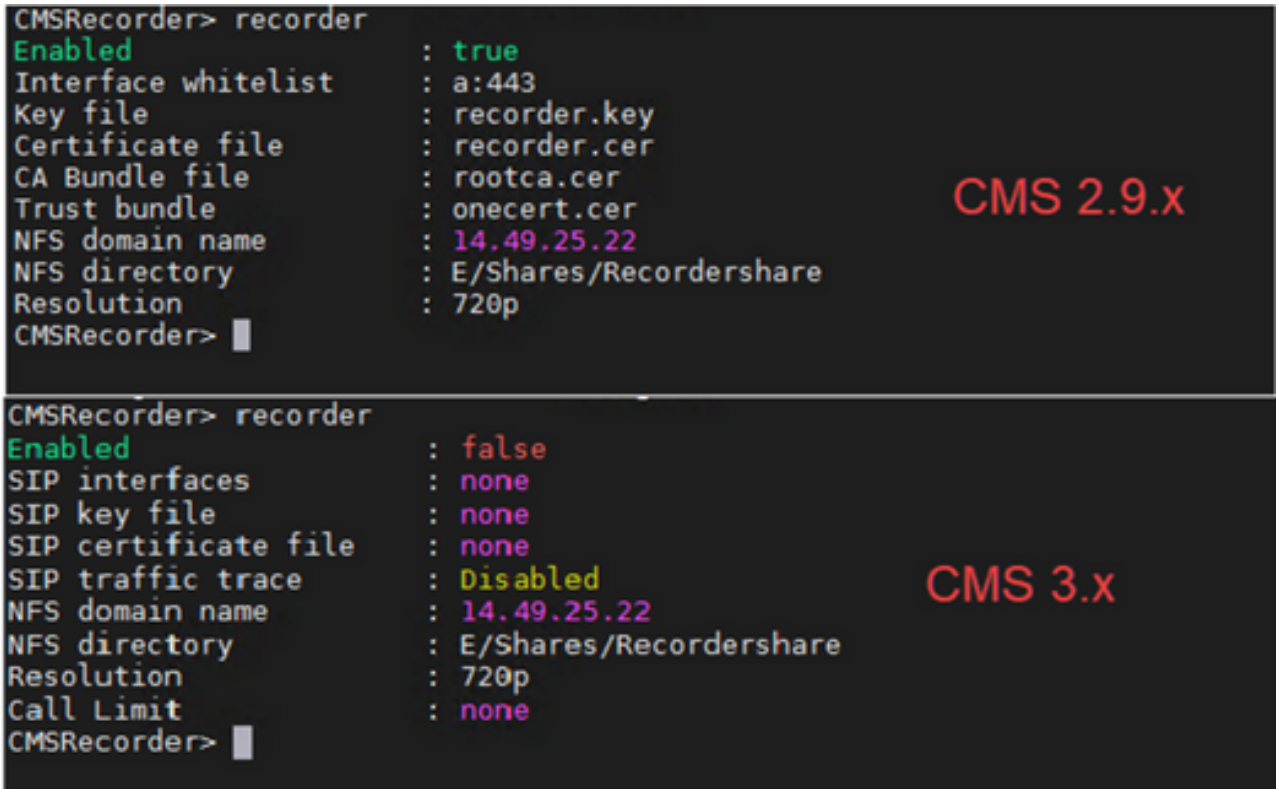
在CMS升级到3.0之前，建议使用“backup snapshot <servername_date>”进行备份，然后登录Callbridge节点上的Webadmin页面以删除所有XMPP设置。 然后，连接到服务器上的MMP，并在通过SSH连接具有xmpp的所有核心服务器上执行以下步骤：

1. xmpp disable
2. XMPP重置
3. xmpp certs none
4. xmpp domain none

录制器

MMP

图中显示了配置记录器时在CMS 2.9.1上看到的配置示例，以及升级到3.0后其外观。



升级后，您必须重新配置录制器：

步骤1:配置SIP侦听接口。

记录器sip监听5060 5061（SIP记录器设置为监听TCP和TLS的接口和端口）。如果不想使用TLS，可以使用“recorder sip listen a 5060 none”)

第二步：配置使用TLS连接的记录器使用的证书。

recorder sip certs <key-file> <crt-file> [crt-bundle](如果没有这些证书，tls服务不会在录制器上启动。记录器使用crt捆绑包验证callBridge证书。)

第三步：配置呼叫限制。

recorder limit <0-500|none>（设置服务器可同时处理的记录数限制）。该表在我们的文档中，记录器限制必须与服务器上的资源一致。)

Table 6: Internal SIP recorder performance and resource usage

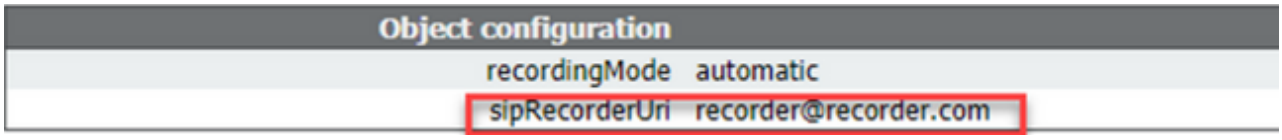
Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

Key point to note (applies to new internal recorder component only):

- Performance scales linearly adding vCPUs up to the number of host physical cores.

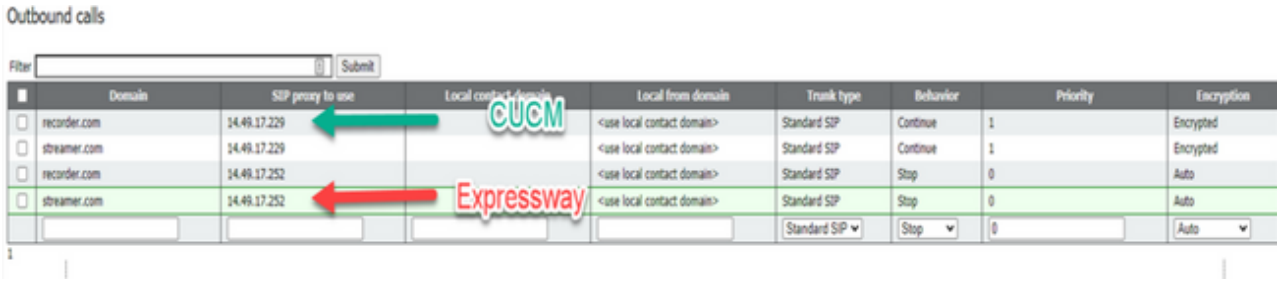
API

在api/v1/callProfiles上，您需要配置sipRecorderUri。这是callBridge在必须开始录制时拨打的URI。此URI的域需要添加到出站规则表，并指向记录器（或呼叫控制）作为要使用的SIP代理。



此图显示在Configuration > Outbound Calls上找到的出站规则上的直接拨号到录制器组件。

此图显示了通过呼叫控制(例如Cisco Unified Communications Manager (CUCM)或Expressway)对录制器组件的呼叫。



注意：如果您将录制器配置为使用SIP TLS，并且呼叫失败，请检查MMP中的callBridge节点，以查看您是否启用了TLS SIP验证。 MMP命令是“tls sip”。 呼叫可能会失败，因为记录器证书不受callBridge信任。 要测试此功能，可使用‘tls sip verify disable’在callBridge上禁用此功能。

多个录音机？

按照说明配置每个规则，并相应地调整出站规则。 如果使用直接记录器方法，请将现有的出站记录器规则更改为行为“继续”，并在前一条规则下添加新的出站规则，其优先级比第一条规则低。 当第一个记录器达到其呼叫限制时，它在此处将488 Unacceptable返回到callBridge，并且callBridge移至下一个规则。

如果要对记录器进行负载均衡，请使用呼叫控制并调整呼叫控制路由，以便它能够向多个记录器发出呼叫。

流转换器

MMP

从2.9.x升级到3.0后，您需要重新配置streamer。

步骤1:配置SIP侦听接口。

streamer sip listen a 6000 6001（SIP streamer设置为侦听TCP和TLS的接口和端口，请严格遵循）。 如果不想使用TLS，可以使用“streamer sip listen a 6000 none”)

第二步：配置使用TLS连接时流转换器使用的证书。

streamer sip证书<密钥文件> <crt文件> [crt捆绑包](如果没有这些证书，tls服务不会在streamer上启动。流转换器使用crt捆绑包验证callBridge证书。)

第三步：配置呼叫限制

streamer limit <0-500|none>(设置服务器可同时处理的流的数量限制。该表在我们的文档中，流转换器限制必须与服务器上的资源一致。)

Table 7: Internal SIP streamer recommended specifications

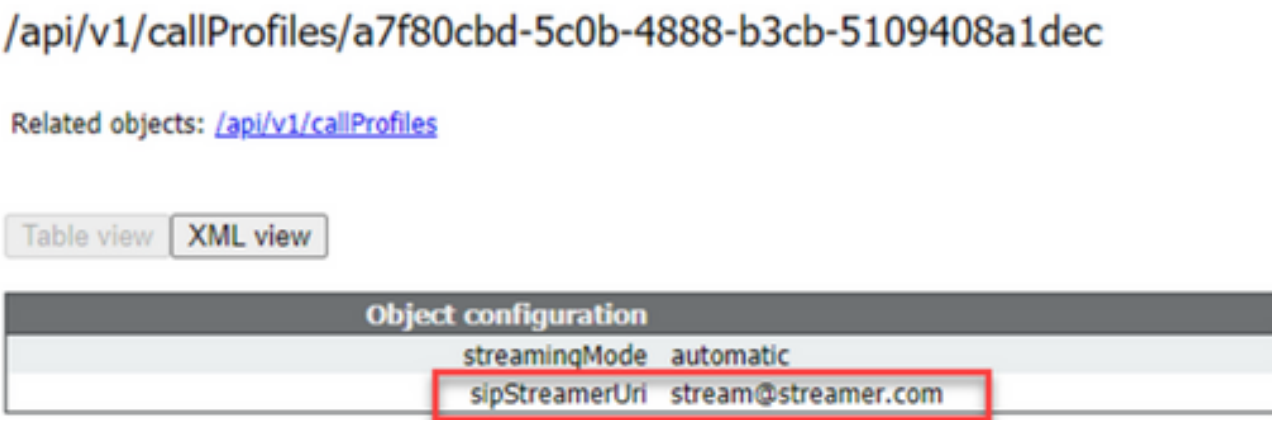
Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

Key points to note (applies to both new internal recorder and streamer components):

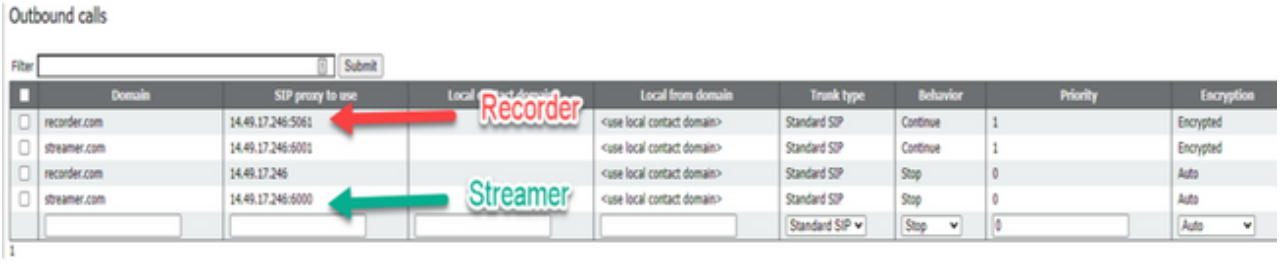
- Number of vCPUs should not oversubscribe the number of physical cores.
- Maximum number of 720p streams supported is 200 regardless of adding more vCPUs
- Maximum number of 1080p streams supported is 150 regardless of adding more vCPUs.
- Maximum number of audio-only streams supported is 200 regardless of adding more vCPUs.

API

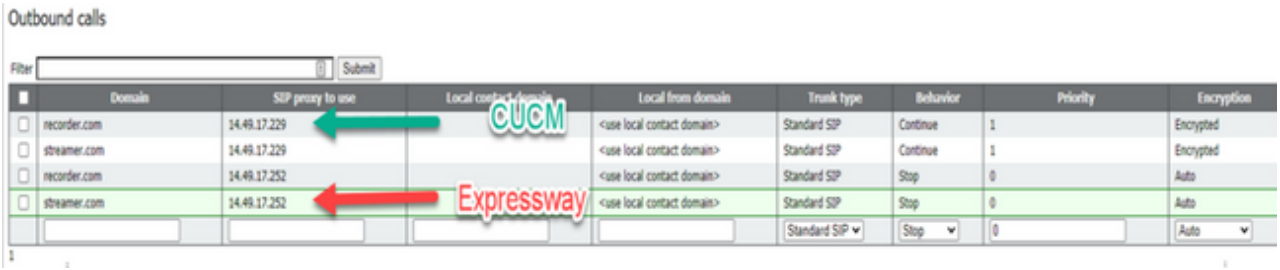
在api/v1/callProfiles上，您需要配置sipStreamUri。这是callBridge在必须启动流传输时拨打的URI。此URI的域需要添加到出站规则表，并指向流转换器（或呼叫控制）作为要使用的SIP代理。



此图显示在Configuration > Outbound Calls上找到的出站规则上的直接拨号到streamer组件。



此图显示了通过呼叫控制(例如Cisco Unified Communications Manager (CUCM)或Expressway)对录制器组件的呼叫。



注意：如果您将流转换器配置为使用SIP TLS，并且呼叫失败，请检查MMP中的callBridge节点，以查看您是否启用了TLS SIP验证。 MMP命令是“tls sip”。 呼叫可能会失败，因为callBridge不信任流转换器证书。 要测试此功能，可使用‘tls sip verify disable’在callBridge上禁用此功能。

多个Streamer？

按照说明配置每个规则，并相应地调整出站规则。 如果使用direct to streamer方法，请将现有的“outbound to recorder”规则更改为行为“Continue”，并在上一个规则下添加新的出站规则，该规则的优先级比第一个规则低1。 当第一个流转换器达到其呼叫限制时，它在此处将488 Unacceptable返回到callBridge，并且callBridge移至下一个规则。

如果要对数据流进行负载均衡，请使用呼叫控制并调整呼叫控制路由，以便它能够向多个数据流发出呼叫。

Expressway注意事项

如果您使用适用于Web代理的Cisco Expressway，则必须确保在CMS升级之前Expressway至少运行X12.6。CMS 3.0需要此许可证才能使Web代理运行并获得支持。

与CMS 3.0配合使用时，Web应用参与者的容量比Expressway有所增加。 对于大型OVA Expressway，预期容量为150个全高清呼叫(1080p30)或200个其他类型呼叫（例如720p30）。您可以通过将Expressway集群来增加此容量，最多6个节点（其中4个用于扩展，2个用于冗余，因此最多600个全高清呼叫，或800个其他类型呼叫）。

Table 3: Cisco Meeting Server web app call capacities – external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway
Cisco Expressway Pair (X12.6 or later)	Full HD	150	150
	Other	200	200

CMS边缘

CMS Edge在CMS 3.1中重新引入，因为它提供的容量比用于外部Web应用会话的Expressway更高。建议采用两种配置。

小型边缘规格

4 GB RAM、4个vCPU、1Gbps网络接口

此VM Edge规格有足够的电源支持单个CMS1000音频和视频负载容量，即48 x 1080p、96 x 720p、192 x 480p和1000音频呼叫。

对于部署，建议每个CMS1000有1台小型边缘服务器，或者每个CMS2000有4台小型边缘服务器。

大型边缘规格

8 GB RAM、16个vCPU、10Gbps网络接口

此VM Edge规格有足够的电源支持单个CMS2000音频和视频容量，即350 x 1080p、700 x 720p、1000 x 480p和3000 x音频呼叫。

对于部署，建议每个CMS2000或每个4 CMS1000有1个大型边缘服务器。

Type of Calls	1 x 4 vCPU VM call capacity	1 x 16 vCPU VM call capacity
Full HD calls, 1080p30 video	100	350
HD calls, 720p30 video	175	700
SD calls, 448p30 video	250	1000
Audio Calls (G.711)	850	3000

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。